Global Investigations Review

The Guide to Cyber Investigations

Editors
Benjamin A Powell and Jason C Chipman

Second Edition

The Guide to Cyber Investigations

Editors:

Benjamin A Powell

Jason C Chipman

Reproduced with permission from Law Business Research Ltd
This article was first published in June 2021
For further information please contact Natalie.Clarke@lbresearch.com

Published in the United Kingdom
by Law Business Research Ltd, London
Meridian House, 34-35 Farringdon Street, London, EC4A 4HL, UK

www.globalinvestigationsreview.com

The information provided in this publication is general and may not apply in a specific situation, nor does it necessarily represent the views of authors' firms or their clients. Legal advice should always be sought before taking any legal action based on the information provided. The publishers accept no responsibility for any acts or omissions contained herein. Although the information provided is accurate as at May 2021, be advised that this is a developing area.

Enquiries concerning reproduction should be sent to: natalie.clarke@lbresearch.com.
Enquiries concerning editorial content should be directed to the Publisher:
david.samuels@lbresearch.com

ISBN 978-1-83862-595-5

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

Acknowledgements

The publisher acknowledges and thanks the following for their assistance throughout the preparation of this book:

ANDERSON MORI & TOMOTSUNE

BAKER MCKENZIE

BCL SOLICITORS LLP

CLIFFORD CHANCE US LLP

COVINGTON & BURLING LLP

CRAVATH, SWAINE & MOORE LLP

RICHARD DENATALE

HUGHES HUBBARD & REED

K&L GATES LLP

KROLL, A DIVISION OF DUFF & PHELPS

BRIAN MCDONALD

QUINN EMANUEL URQUHART & SULLIVAN, LLP

ROPES & GRAY LLP

WILMER CUTLER PICKERING HALE AND DORR LLP

Publisher's Note

The Guide to Cyber Investigations is published by Global Investigations Review – the online home for all those who specialise in investigating and resolving suspected corporate wrongdoing.

It aims to fill a gap in the literature and provide an in-depth guide to every aspect of preparing for and dealing with data breaches and other cyber incidents. These incidents can be challenging, to say the least.

As such it is a companion to GIR's larger reference work, *The Practitioner's Guide to Global Investigations* (now in its fifth edition), which walks readers through the issues raised, and the risks to consider, at every stage in the life cycle of a corporate investigation, from discovery to resolution.

The Guide to Cyber Investigations takes the same holistic approach, going through everything to think about before, during and after an incident. We suggest both books be part of your library – *The Practitioner's Guide* for the whole picture and *The Guide to Cyber Investigations* as the close-up.

The Guide to Cyber Investigations is supplied to all GIR subscribers as a benefit of their subscription. It is also available to non-subscribers in online form only, at www.globalinvestigationsreview.com.

The publisher would like to thank the editors for their energy and vision. We collectively welcome any comments or suggestions on how to improve it. Please write to us at insight@globalinvestigationsreview.com.

Contents

Part II

Jurisdictional, Regional and Sectoral Nuances

15

Japan

Daisuke Yamaguchi, Takashi Nakazaki and Atsushi Nishitani[1]

Key cybersecurity standards and requirements

There are cybersecurity standards to be complied with, and notifications detailing such requirements have been issued by various governmental departments in Japan. For instance, the Ministry of Economy, Trade and Industries (METI) issued the Information Security Management Standards (the METI Standards) (METI Public Notice No. 112 of 2003) in 2003 and updated them in 2016 (METI Public Notice No. 37 of 2016). The Standards were formulated in accordance with international standards and practices. Furthermore, by incorporating the responses to opinions from external experts and public comments, etc., METI included the associated article numbers specified in ISO 27001; added details to the simplified descriptions found in ISO 27001; and, by including other measures, the METI Standards were formulated so that they would contribute to the smooth operation of the information security audit system. The METI Standards consist of two parts: management standards and control measures standards. The management standards part provides for the necessary items for information security management plan-do-check-act procedures, and is based on JIS Q 27001:201, while the control measures standards part provides for possible control measures to be implemented in establishing information security management and is based on JIS Q 27001:2014 Appendix A and JIS Q 27002:2014.

Furthermore, in 2018, METI formulated two additional cybersecurity-related standards: Information Security Service Standards and Standards for Examination-Registration Organizations for Information Security Services.

The Information Security Service Standards overlook:

- information security inspection;
- vulnerability diagnosis;

1 Daisuke Yamaguchi and Atsushi Nishitani are partners and Takashi Nakazaki is a special counsel at Anderson Mori & Tomotsune.

- digital forensics; and
- security monitoring and operation services.

The standards stipulate a certain level of quality to be maintained in the respective services:
- technical requirements (e.g., qualification requirements and explicit indication of specifications); and
- quality management requirements, (e.g., allocation of quality managers to appropriate duties, development of quality management manuals, and where service providers have introduced procedures for maintaining and improving quality).

Examination-registration organisations are bodies established to examine applicants as private information service providers, regarding whether or not the providers' services comply with the Information Security Service Standards, and to register appropriate providers. The Standards for Examination-Registration Organizations for Information Security Services stipulate rules that such organisations should observe, including fairness in examination and general rules for organisation management and examination procedures.

Sectoral standards

Telecommunication sector

The Ministry of Internal Affairs and Communications established the Safety and Reliability Standards of Information and Communication Network in 1987. The Security and Reliability Standards have been amended several times and the latest version was released in 2020. The Security and Reliability Standards consist of two parts (facilities standards and management standards) and contain software measures, information security measures, earthquake countermeasures, power outage measures and various other measures.

Financial sector

The Financial Services Agency (FSA) issued a summary of its policies to strengthen cybersecurity in the financial sector in 2015 and updated it in 2018. The FSA plans to:
- promote continuous dialogue with financial institutions to understand their cybersecurity risks;
- improve information sharing among financial institutions;
- implement cyberattack drills in which financial institutions, the FSA and other public authorities participate; and
- develop human resources specialising in cybersecurity, and also respond to new issues such as accelerated digitalisation and international discussions.

The FSA's guidelines require banks to, among other things, establish an organisation to handle emergencies, designate a manager in charge of cybersecurity, prepare multi-layered defences against cyberattacks and implement a periodic assessment of cybersecurity.

Summary of breach notification rules

There are no general reporting requirements of security breach under Japanese law. As for security breach of personal data, there will be reporting requirements of security breach under the Act on the Protection of Personal Information (Act No. 57 of 2003, as amended) (APPI) from April 2022; however, there are currently no legal requirements of reporting to the authorities under the APPI.

The Amendment to APPI in 2021 will require businesses to report to the Personal Information Protection Commission and notify subjects (who have suffered due to the breach) when a business recognises that there is or might possibly be a security breach that is likely to 'harm the rights and interests of individuals'. Businesses will be required to report to the relevant authority in specified time frames and to inform affected individuals in a timely manner. Reporting will be required in the following scenarios:

1 leakage of special category data (similar to sensitive data);
2 damage to property or potential risk of damage to property;
3 intentional violation of the law, such as unauthorised access; and
4 the breach affects at least 1,000 data subjects.

The amendment requires the reporting to be done twice; in other words, a prompt report must be submitted and a more detailed report submitted thereafter (the latter report must be filed within 30 days of recognising a security breach as described above in (1), (2) and (4), and within 60 days of recognising a security breach described above in (3)). Even on the occurrence of any of the events described above, a business need not report a security breach to the Personal Information Protection Commission if it has implemented sufficient security management measures for protecting the rights and interests of individuals. A typical example of sufficient security management measures would be advanced encryption. This amendment will come into effect on 1 April 2022.

Also, there are reporting requirements in some business sectors, such as the telecommunications sector and the financial sector. As for the telecommunications sector, the Telecommunications Business Act (Act No. 86 of 1984, as amended) (TBA), which is the main legislation governing that sector, requires a telecommunications carrier to report a security breach to a Minister at the Ministry of Internal Affairs and Communication (MIC). Article 28 of the TBA specifies three cases that must be reported:

1 when a telecommunications carrier suspends its telecommunications operations in part pursuant to the provisions of Article 8, Paragraph (2) of the TBA;
2 a violation of secrecy of communications; or
3 any other serious accident specified by order of MIC has occurred with respect to telecommunications operations.

As for item (2), many violations of secrecy of communications cause data breach of personal data belonging to telecommunication service users. Such reporting should be based on the guidelines on data breach reporting in the telecommunications sector, and such reporting should be carried out in accordance with the guidelines.[2] As for item (3), those serious

2 www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/denkitsushin_rouei.html.

accidents are specified in Article 58 of the Ordinance for Enforcement of the TBA. Details are available in the 'Guidelines for Application of the Telecommunications Business Act and Related Regulations on Telecommunications Accidents and Incidents.'[3] A telecommunications carrier is required to report the incident to MIC promptly after its occurrence. In addition, the carrier is required to report details of the incident to MIC within 30 days from its occurrence. The detailed report must include the following items:

- the date and time when the incident occurred;
- the date and time when the situation was remedied;
- the location where the incident occurred (the location of the facilities);
- a summary of the incident and which services were affected by the incident;
- a summary of the facilities affected by the incident;
- details of the events or indications of the incident, the number of users affected and the affected service area;
- measures taken to deal with the incident, including the persons who dealt with it, in chronological order;
- causes that made the incident serious, including how the facilities have been managed and maintained;
- possible measures to prevent similar incidents from happening;
- how the telecoms carrier responded to inquiries from users and how it notified users of the incident;
- internal rules in connection with the incident;
- if the telecoms carrier experienced similar incidents in the past, and a summary of past incidents;
- the name of the manager of the telecoms facilities; and
- the name and qualifications of the chief engineer of the telecoms facilities.

As for the financial sector, the FSA (the main authority supervising the financial sector) issues various guidelines for supervising financial sectors such as banks and insurance companies. For major banks, the FSA issues the Comprehensive Guidelines for Supervision of Major Banks, etc. The Guidelines specify that the FSA requires banks to report a cybersecurity incident immediately after becoming aware of it. The report must include the following items:

- date and time when the incident occurred and the location where the incident occurred;
- a summary of the incident and which services were affected by it;
- causes of the incident;
- a summary of the facilities affected by the incident;
- a summary of damages caused by the incident, and how and when the situation was remedied or will be remedied;
- any effect on other business providers;
- how the bank responded to inquiries from users and how it notified users, public authorities and the public; and
- possible measures to prevent similar incidents from occurring.

3 www.soumu.go.jp/main_content/000743122.pdf.

The government encourages each business industry to share security information among the relevant industry groups. Apart from reporting to the authorities, there are many Information Sharing and Analysis Centers (ISACs) in various business sectors, including the financial sector and the ICT sector. Many ISACs have been established, such as Financials ISAC Japan, ICT ISAC Japan, Japan Automobile ISAC, Software ISAC and Japan Electricity ISAC. Several business sectors have established ISACs, and encourage the relevant industry members to share security information with them. For example, Financials ISAC Japan has two core functions:

- 'collective intelligence', which focuses on intelligence sharing between members in relation to any daily incident or exposed vulnerability; and
- 'resource sharing', which, through cooperative action, pools resources to promote consideration of strategies to deal with shared issues.

A Financial ISAC consists of over 400 financial institutions as regular members and around 30 IT vendor companies as affiliate members. Financial ISACs hold cyberattack drills regularly. If a Financial ISAC finds important information, 100 members will be committed to conducting a variety of activities aimed at building a solid foundation to promote customers' peace of mind, safety and security, which lies at the heart of Japan's financial system.

Best practices for cyber-incident response

Cybersecurity Management Guidelines Version 2.0, issued by METI, indicates best practices for a cyber-incident response. The Guidelines insist that it is important to develop a cybersecurity incident response team, and that relevant procedures should be put in place to establish a response structure within the organisation (a computer security incident response team (CSIRT), etc.) to identify the scope of impact and damage; take initial action to prevent further damage and implement measures to prevent similar incidents from recurring; decide what information should be reported to whom in the case of an emergency; and support management to report that information to internal and external stakeholders appropriately. This is a checklist for best practices:

- Conserve evidence such as various logs and devices infected with malware after being victimised by a cyberattack, for swift identification and analysis of the cause of damage, giving directions to employees to cooperate with relevant organisations for joint investigation. In investigating the cause of an incident, the Guidelines recommend referring to Appendix C of the Guidelines, 'Items to organise within the organisation for the occurrence of incidents.'
- Execute drills in preparation for cyberattacks including developing measures to prevent similar incidents from recurring and reporting to relevant government agencies. The Guidelines recommend considering consulting external experts as necessary for measures to prevent recurrence.
- Prepare a list of emergency contacts (security vendors, etc.) and a list of organisations to disclose information to, including external parties, and share those lists with incident response members.
- Calculate the impact of first response on regular business operations and, based on that, make arrangements in advance with other divisions of the organisation (HR, sales, etc.) for emergencies.

- Check relevant laws and regulations and procedures to fulfil obligations described in the laws and regulations.
- Report to management the damage status and impact to other companies owing to the incidents.

Cybersecurity and Incident response trends:

Increasing number of cybersecurity incidents

As in many other countries, the number of cyberattacks found in Japan has been increasing rapidly. In 2019, 2,960 cases of unauthorised access were recognised in Japan (this is the number of cases reported to the National Police Agency),[4] which was increased by 99.2 points from the previous year. The number of phishings reported to the Council of Anti-Phishing Japan was 55,287 in 2019, which is 2.8 times larger than in 2018.[5]

On 18 December 2020, METI issued a news release 'Alerts to Company Executives to be Issued to Encourage them to Enhance Cybersecurity Efforts in Light of Situations of Recent Cyberattacks'.[6] METI warned in the release that:

- there had been a rapid expansion of diversity of cyberattack patterns targeting supply chains in which SMEs are involved;
- there had been a rapid increase in the number of ransomware victims, regardless of size of enterprise; and
- overseas connections were becoming targets of attackers wishing to steal highly sensitive information.

Challenges in Japan

One of the most crucial issues in cybersecurity areas in Japan is the shortage of cybersecurity professionals. According to a research report,[7] 86.2 per cent of Japanese companies think that they do not have enough human resources for cybersecurity, compared with 16.1 per cent of US companies and 17.1 per cent of Australian companies. Another research report[8] showed that only 22.8 per cent of Japanese companies (among 534 samples) have at least one full-time CSIRT member.

Lack of cybersecurity professionals causes various problems for Japanese companies and sometimes prevents them from quickly finding, responding to and recovering from cybersecurity issues.

4 National Public Safety Commission, Minister of Internal Affairs and Communications and Minister of Economy, Trade and Industry, 'Status of occurrence of unauthorised access and status of research and development on technologies for access-control functions' dated 5 March 2020.

5 Council of Anti-Phishing Japan, 'Phishing Report 2020' dated 23 June 2020.

6 www.meti.go.jp/english/press/2021/1218_001.html.

7 NRI SecureTechnologies, Ltd, 'NRI Secure Insight 2020' published on 15 December 2020.

8 Information-technology Promotion Agency, 'Report on survey of CISO, etc. and promotion of security measures of companies' dated 25 March 2020.

Regulatory consideration

Legal framework

The Basic Act on Cybersecurity (Act No. 104 of 2014, as amended) (BAC), which came into effect in January 2015, was the first act focusing on cybersecurity issues in Japan. The BAC provides the basic framework of government policies of cybersecurity, including basic principles; responsibilities of the Japanese government and local governments; and essential matters for cybersecurity-related policies.

The Cybersecurity Strategy of the Japanese government is determined and published pursuant to the BAC; however, the BAC does not intend to regulate the activities of private companies and individuals directly. Concurrent with enforcement of the BAC, the Cybersecurity Strategic Headquarters (CSH) and National Center of Incident Readiness and Strategy for Cybersecurity (NISC) were established in the Cabinet to promote various cybersecurity related policies and coordinate with various stakeholders in public and private.

Specific regulations and legal responsibilities regarding cybersecurity issues are stipulated in the individual laws and regulations. The following are important laws regarding cybersecurity in Japan.

Personal Data Protection Regulations

The APPI regulates handling of personal data mainly in private sectors. The APPI requires personal information-handling business operators to take necessary and appropriate action for the security control of personal data, including preventing the leakage, loss or damage of its handled personal data. The Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure (Act No. 27 of 2013, as amended) (the 'My Number Act') also requires those who are handling of Individual Numbers[9] to take necessary measures to ensure the appropriate management of Individual Numbers, such as preventing the leakage, loss or damage of Individual Numbers.

The main regulator for the APPI and the My Number Act is the Personal Information Protection Commission (PPC), the independent regulatory body established based on the APPI. The PPC is responsible for establishing the Basic Policy on Protection of Personal Information and overseeing compliance of the APPI and the My Number Act. The PPC has issued guidelines on the APPI, providing detailed guidance on the scope and interpretation of the APPI. In addition to the PPC guidelines, relevant administrative authorities have issued guidelines for specific areas, including finance, medical, telecommunication and employment and welfare sectors. Although those guidelines are not legally binding documents, they are generally accepted by companies and legal practitioners.

Other important laws and regulations on cybersecurity

Under the Companies Act (Act No. 86 of 2005, as amended), it is understood that directors of a Japanese company have a duty to establish appropriate cybersecurity measures as part of the internal control system of the company. Breach of such duty could face civil liability (including a shareholder derivative suit) against directors.

9 The Individual Number (My Number) is a unique 12-digit number for each individual provided by the government, and used in social insurance, tax and disaster countermeasure areas within Japan.

In connection with cybersecurity management of companies, METI and the Information-technology Promotion Agency jointly published the Cybersecurity Management Guidelines in 2015, and the latest revised version (Version 2.0) was published in 2017.[10] The guidelines are aimed at the corporate management of major companies as well as small and medium-sized companies and include, from the viewpoint of protecting companies from cyberattacks, the three principles that management need to recognise and 10 important items that management should direct their executive in charge (CISO) to observe in implementing cybersecurity measures. The guidelines themselves are not legally binding, but whether they are followed or not may be an important element to consider for compliance of duty of directors (see the 'Litigation consideration' Section for details).

For the telecommunications sector, the TBA requires telecommunications carriers to maintain telecommunications facilities in conformity with the technical standard specified by the Order of the Ministry of Internal Affairs and Communications, and the technical standard includes detailed cybersecurity related requirements. From April 2020, certain security measures for IoT devices have been included in the technical standards.

As to criminal liability, the Act on Prohibition of Unauthorised Computer Access (Act No. 128 of 1999, as amended) prohibits unauthorised access to computer systems, as well as illegal collection of IDs and passwords of other people and provision thereof. Violators could face up to three years in prison or a ¥1 million fine.

The Unfair Competition Prevention Act (Act No. 47 of 1993, as amended) and Copyright Act (Act No. 48 of 1970, as amended) prohibits provision of software or devices exclusively for the purpose of circumvention of technological restriction or protection measures (i.e., copy control or access control measures). Violators could face up to three years in prison or a ¥3 million fine (under the Copyright Act), or up to five years in prison, a ¥5 million fine, or both (under the Unfair Competition Prevention Act). Acquisition of a trade secret by act of fraud (including unauthorised access stipulated in the Act on Prohibition of Unauthorised Computer Access) shall be subject to up to 10 years in prison, or a ¥10 million yen fine, or both.

The Penal Code (Act No. 45 of 1907, as amended) also prohibits certain cyberattack-related activities including:

- making or distribution of computer viruses (up to three years in prison or a ¥500,000 fine);
- skimming of credit-card information (up to three years in prison or a ¥500,000 fine);
- obstruction of the business of another by interfering with the operation of a computer or damaging electromagnetic record (up to five years in prison or a ¥1 million fine); and
- computer fraud by creating a false electromagnetic record, imputing false data or giving unauthorised commands (up to 10 years in prison).

Cybersecurity regulators

As the CSH and NISC are mainly responsible for strategy planning and coordination, there is no one-stop regulator on cybersecurity matters in Japan. As to the data protection issues, the PPC is the main regulator and has the authority to provide guidance and advice; request reports; conduct on-site inspections, offer recommendations and give orders to governmental

10 www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0_en.pdf.

institutions and business operators who handle specific personal information. For other specific areas and industries, the ministry with jurisdiction over the applicable laws and regulations should be the main regulator (for example, the MIC for telecommunications business).

Litigation consideration

A company that has suffered a cyberattack may be sued by an affected business partner or individual, or a lawsuit may be instituted by a shareholder against the company's directors and officers.

Suit against a company by a business partner or individual who has suffered damage

Claim for damages based on breach of contractual provisions

For example, a business partner enters into a business alliance agreement with Company A and discloses confidential information (technical information, customer information, etc.) to Company A. If the aforementioned confidential information is stolen as a result of a cyberattack by a foreign hacker on Company A's systems, and the business partner suffers damages thereby, the business partner may file a claim for damages against Company A based on the breach of contractual provisions (i.e., breach of obligations to safeguard and protect confidential information of the business partner, obligations for secure management of information, etc.).

Under the Civil Code of Japan, to establish breach of contract, one must prove:

- the fact that there was a default by a party;
- the reasons for which the defaulting party is to be held responsible; and
- the damage caused (Article 415 of the Civil Code).

The extent of damages that can be claimed will depend on the limitation on the compensation for damages agreed to by both the parties in the contract. However, in the absence of such a limitation clause, in addition to ordinary damages, special damages that could have been foreseen at the time of the default are also covered under the Civil Code (Article 416, Paragraph 2).

Therefore, in addition to the damages arising from the theft of technical information, in the event that the amount of sales of the products using such technical information falls, Company A will be liable to compensate the business partner for the decrease in sales as special damages.

Claim for damages based on tort

For example, if a company has an individual's personal information stolen and there is no contractual relationship between the individual and the company, the individual may file a claim under tortious liability against the company.

The facts required for claiming damages based on tort are: intention and negligence; illegality (infringement); damage; and causality (Article 709 of the Civil Code).

Unlike in the United States, one cannot claim for punitive damages in Japan.

Suit instituted by a company's shareholders against directors and officers

If a company suffers damages as a result of a cyberattack due to insufficient cybersecurity systems being put in place to protect confidential data, shareholders may institute a derivative suit against the company's directors and officers for breach of their duty of care.

At present, there have been no cases of shareholders' lawsuits being instituted for damages owing to failure to provide cybersecurity systems in Japan. However, with regard to theft of personal information, the Benesse Group experienced a personal information leak: an employee of a business operator entrusted with the management of personal information of customers illegally acquired or sold personal information. A shareholder lawsuit was instituted against the director of a holding company of the Benesse Group, for compensation of ¥26 billion.

Rejecting the appellant request of the shareholders, the appeals court found that:

- the Benesse Group had established various rules such as the Business Corporation Management Rules and, based on these, conducted a certain level of business management through participation in personnel affairs and business planning; risk assessment and examination of the group as a whole; reading of various reports, etc., to ensure compliance with laws and regulations; and established and operated an internal control system as a group of companies; and
- there was no proof that, considering the current practice of domestic listed companies at the time of this case, the establishment and operation of the Benesse Group's internal control system was below the standard.[11]

As can be seen from the above trial case, the establishment of a system to protect personal information or to promote cybersecurity constitutes a part of the duties of directors to establish and operate internal control systems (Article 348, Paragraph 3, Item 4 of the Companies Act).

The three principles and the 10 important items set forth in the Cybersecurity Management Guidelines represent a specific model of the philosophy and measures of the internal control system to be established in relation to a cybersecurity system. To prevent directors from being sued for violation of their managerial obligation of due care, it is necessary to establish and check the cybersecurity system of the company, and to establish a system that does not fall below the standard of current practice as mentioned above, especially pertaining to the above three principles and the 10 important items.

Types of threats or threat actors: criminal, nation-state, insider (intentional and accidental)

Criminals (hackers), the state and insiders are considered to be the main actors who conduct cyberattacks.

Offender

In Japan, criminals engage in illegal information access or theft of company assets through methods such as malware attacks, ransomware attacks, denial of service, distributed denial

11 Appeal court decision by the Okayama branch of the Hiroshima High Court, 18 October 2019.

of service, phishing emails, business e-mail fraud and unauthorised access or alteration of websites.

In 2015, the terminals of employees of the Japan Annuity Payments Organization were illegally accessed by means of sending an e-mail with a virus from outside, targeting the organisation; 1.25 million people's personal information (basic pension number, name, date of birth, address) were leaked.

Nation

In the *Coincheck* incident, about ¥58 billion worth of virtual currency NEM was stolen in January 2018. The *Coincheck* incident was carried out by an overseas hacker. Coincheck put the 'private key' used for transactions, such as remittance of virtual currency, in a hot wallet connected to the internet (a wallet disconnected from the internet is called a cold wallet). The private key was allegedly stolen by an outside hacker through the internet, and a large number of NEMs were stolen. The NEM Foundation, in cooperation with engineers, placed tracking mosaics on the stolen NEM wallets, keeping them under constant surveillance to prevent perpetrators from converting the stolen NEMs into other currencies. However, even with this tracking method, if the perpetrator exchanged the NEMs for another currency in the highly anonymous network called the Dark Web, identification of the perpetrator who stole the NEMs would be extremely difficult.

Insiders

Damages incurred by a company may be caused by intentional fraud or human error of the insider. Typical examples of insider fraudulent activities are as follows:

- employees send important information to personal addresses with email attachments;
- employees use apps installed on company leased smartphones to connect to the company's computer and take confidential information outside using Wi-Fi;
- removal or exchange of confidential information by a system administrator;
- leakage of customer information by an outsourced employee;
- removal or exchange of confidential information by a homeworker;
- removal of confidential information by retirees; and
- actions that are not intentional, for example, when leakage of personal information is caused due to human error such as inadvertent erroneous transmission of emails.

Damages suffered by a company due to fraud by insiders include the loss of customer information, business information and technical information that the company manages as its trade secret; economic loss resulting from liability for damages to customers; and reputational damage resulting from loss of credibility as a company.

Recent trends in types of cyberthreat, detection time, etc.

Because hacking from overseas was raised as a possibility with regard to the *Coincheck* incident (see above), administrative supervision and legislation in Japan alone cannot adequately deal with such an incident. The Financial Stability Board, which comprises financial supervisory authorities in major countries, created a contact list to help local authorities in charge of virtual currency administration in each country to understand their responsibilities. In

addition, if any cybercrime actually occurs, a system must be established to identify the culprit through international cooperation among investigative authorities and engineers in each country, and to investigate and recover assets outside Japan.

Appendix 1

About the Authors

Daisuke Yamaguchi
Anderson Mori & Tomotsune

Daisuke Yamaguchi is a partner at Anderson Mori & Tomotsune in the corporate group. He has been engaged in various cybersecurity and AI-related matters including crisis management regarding cyberattacks, as well as various corporate matters. He is also in charge of the firm's information technology and services and legal-tech, and is a member of CSIRT.

Takashi Nakazaki
Anderson Mori & Tomotsune

Takashi Nakazaki is a special counsel at Anderson Mori & Tomotsune in the IP and technology group, with broad experience in the areas of data protection, privacy, big data and IoT. He has been engaged in various cybersecurity and AI-related matters including crisis management due to cyberattacks. In addition, he regularly assists the Japanese government in cyber law and data protection areas, including the 'AI & Data Contracts Guidelines' and 'AI Governance'. Mr Nakazaki leads the technology law committee of the International Bar Association as vice chair.

Atsushi Nishitani
Anderson Mori & Tomotsune

As a partner at Anderson Mori & Tomotsune, Atsushi is in charge of crisis management and corporate matters for the firm and its clients, including cross-border cases, since he has considerable experience in advising clients in Tokyo and New York at one of the largest Japanese trading corporations. Among other things, he actively engages in various types of fraud investigations and asset tracing and recovery, including cyberattacks, financial fraud and quality-test fraud.

Anderson Mori & Tomotsune
Otemachi Park Building
1-1-1 Otemachi
Chiyoda-ku
Tokyo 100-8136
Japan
Tel: +81 3 6775 1000
atsushi.nishitani@amt-law.com
daisuke.yamaguchi@amt-law.com
takashi.nakazaki@amt-law.com
www.amt-law.com

Data breaches and similar incidents pose a unique challenge – those targeted must both respond and investigate simultaneously. It is an art that is impossible without preparation.

Businesses wishing to prepare will find this volume, *The Guide to Cyber Investigations*, invaluable. It identifies every issue to consider when creating a response template and implementing it, giving both the law and plenty of practical and tactical advice.

Written by leading contributors, all with broad experience of serious data incidents, it is an indispensable desktop guide and a worthy companion to GIR's larger volume on cross-border investigations, *The Practitioner's Guide to Global Investigations*.

Visit globalinvestigationsreview.com
Follow @giralerts on Twitter
Find us on LinkedIn

an LBR business

ISBN 978-1-83862-595-5